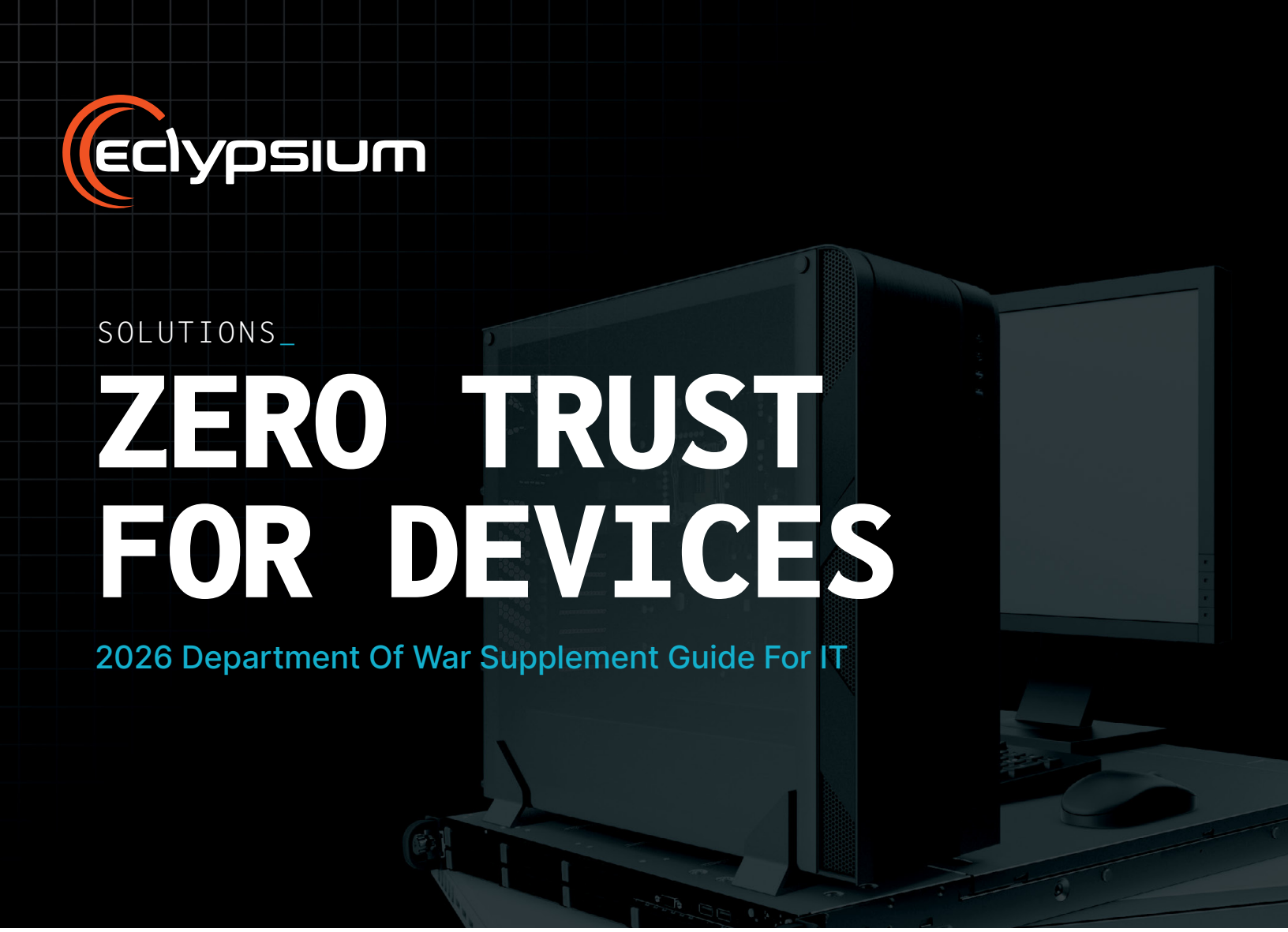


SOLUTIONS_

ZERO TRUST FOR DEVICES

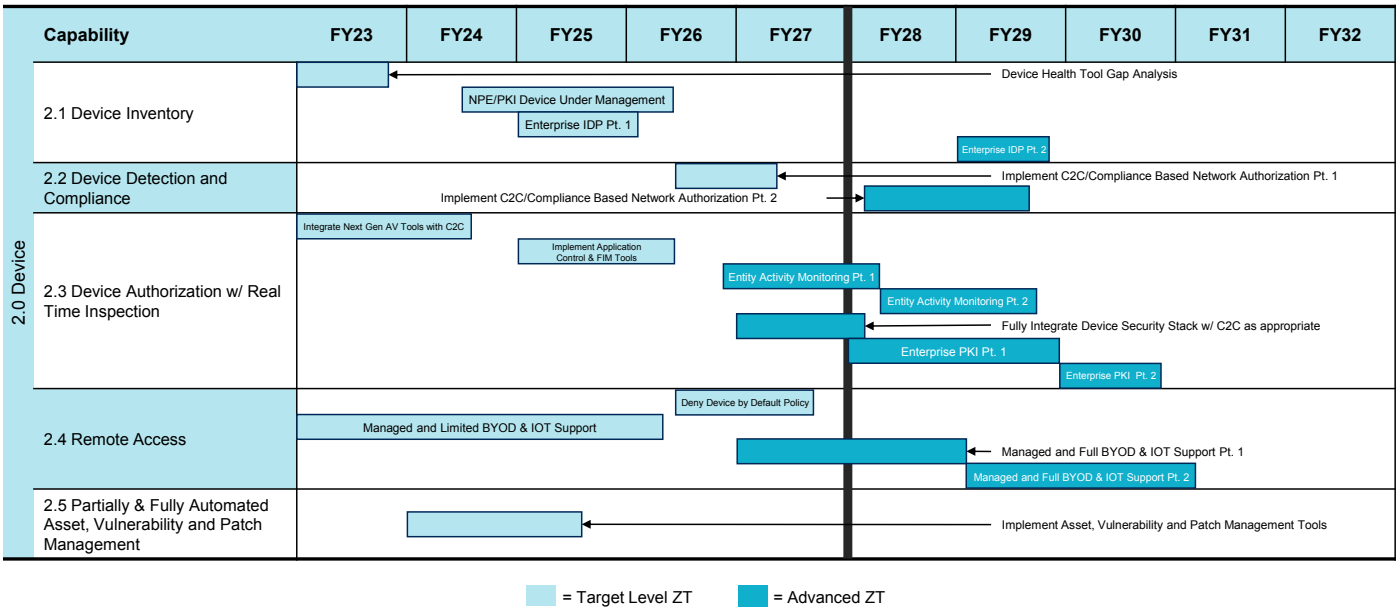
2026 Department Of War Supplement Guide For IT

This supplement extends Zero Trust for Devices (Federal Agencies) publication by aligning device-centric Zero Trust outcomes to Department of War (DoW) Zero Trust Target Level Activities with a 2026 execution horizon. DoW Components are expected to reach Target Level Zero Trust by the end of FY2027 (September 30, 2027)—which makes 2026 the critical year to operationalize controls, close gaps, and produce measurable evidence of progress. Eclypsium is partnering with agencies now to define and implement the hardware and firmware security requirements needed to stay on track.

Why 2026 Matters_

The DoW Zero Trust Capability Execution Roadmap provides a FY23–FY27 implementation timeline toward Target Level Zero Trust, making FY2026 a key execution year for standing up enterprise inventories, deny-by-default enforcement, and continuous device compliance/authorization capabilities. The Device pillar schedule is effectively front-loaded—multiple Target Level device activities are expected to be implemented and matured across FY24–FY26—so many device outcomes must be operational well before the end-of-FY27 deadline to avoid downstream schedule risk.

Figure 1 – Zero Trust Capability Baseline Timeline - Device Pillar



The roadmap launched in FY2023, and FY2025 highlighted common scaling challenges. As a result, FY2026 becomes the last realistic window to procure, integrate, and validate the tools and telemetry needed to demonstrate measurable Target Level progress—rather than relying on policy updates alone.

How Eclypsium Can Help?

Eclypsium helps agencies accelerate progress toward Zero Trust Target Level Activities by providing authoritative device trust signals—firmware/component inventory, integrity verification (known-good baselines), vulnerability/patch posture, and drift detection—that traditional OS-level tools often miss. These signals can be managed within the Eclypsium platform, or they can be integrated into C2C/NAC/ZTNA, UEM, and SIEM/XDR workflows to support continuous verification, risk-based authorization, and measurable Target Level progress.

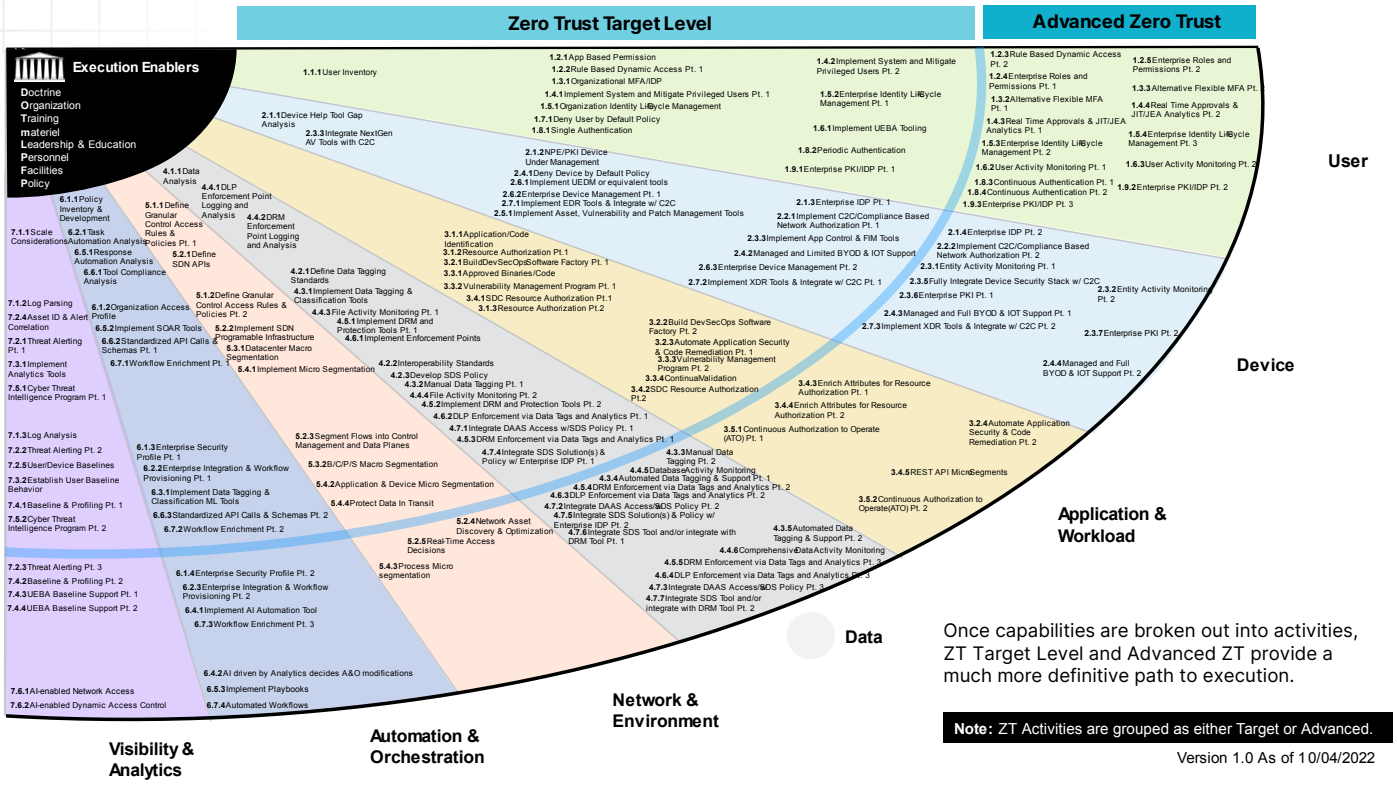


Figure 21 -DoW Zero Trust Activities

Eclypsium can help DoW Components achieve a Zero Trust End State more quickly by supporting 30 of the 91 DoW Target Level Activities.

Activities Supported by Eclypsium_

ID #	Activity Name	How Eclypsium Supports the Activity
	User	
1.2.1	**Implement App Based Permissions per Enterprise**	Eclypsium provides device/firmware trust signals that inform IdP/ICAM/PAM to achieve the activity outcomes
1.2.2	**Rule Based Dynamic Access Pt 1**	On-demand device Eclypsium inquiries provide device/firmware trust signals that inform IdP/ICAM/PAM to achieve the activity outcomes
1.3.1	**Organizational MFA/IDP**	Eclypsium complements MFA/IdP deployments by adding device trust context to authentication workflows—verifying device integrity and firmware risk posture so critical applications can require additional controls when the device is not in a known good state.

ID #	Activity Name	How Eclypsium Supports the Activity
	Device	
2.1.1	**Device Health Tool Gap Analysis**	Eclypsium provides device/firmware health visibility (inventory + integrity/ vulnerability posture) that enables device health gap analysis.
2.1.2	**NPE/PKI, Device under Management**	Eclypsium provides firmware/device posture evidence, along with the hardware root of trust required for the DoD to securely issue X.509 certificates to managed devices.
2.1.3	**Enterprise IDP Pt1**	Eclypsium provides authoritative device/firmware posture (integrity, vuln/patch, baselines) used for enforcement/monitoring.
2.2.1	**Implement C2C/ Compliance Based Network Authorization Pt1**	Eclypsium supports by supplying authoritative device/firmware posture (integrity, vuln/patch, baselines) used for enforcement/monitoring.
2.3.3	**Implement Application Control & File Integrity Monitoring (FIM) Tools**	Eclypsium application control and FIM outcomes by delivering integrity monitoring for the pre OS/firmware layer (e.g., unauthorized firmware modifications, risky configuration changes, baseline drift) and exporting those findings to endpoint security and compliance workflows.
2.3.4	**Integrate NextGen AV Tools with C2C**	Eclypsium provides EPP and EDR functionalities below the operating system, providing visibility into the firmware-level and signatureless threats that traditional endpoint tools overlook. Eclypsium supports by supplying authoritative device/firmware posture (integrity, vuln/patch, baselines) used for enforcement/monitoring.
2.4.1	**Deny Device by Default Policy**	Eclypsium supports by supplying authoritative device/firmware posture (integrity, vuln/patch, baselines) used for enforcement/monitoring.
2.4.2	**Managed and Limited BYOD & IOT Support**	Eclypsium supports by supplying authoritative device/firmware posture (integrity, vuln/patch, baselines) used for enforcement/monitoring of BYOD/IoT.
2.5.1	**Implement Asset, Vulnerability and Patch Management Tools**	Eclypsium provides device firmware-layer vulnerability and patch posture. Eclypsium also provides firmware patch management.
2.6.1	**Implement UEDM or equivalent Tools**	Eclypsium supports by supplying authoritative device/firmware posture (integrity, vuln/patch, baselines) used for enforcement/monitoring.
2.6.2	**Enterprise Device Management Pt1**	Eclypsium provides enterprise device management by delivering continuous firmware-layer trust telemetry (inventory, integrity, drift, and risk posture) and configurable device profiles that drive compliance evaluation and remediation workflows and security automation platforms
2.6.3	**Enterprise Device Management Pt2**	Eclypsium provides enterprise device management by delivering continuous firmware-layer trust telemetry (inventory, integrity, drift, risk posture, and compliance) and that can be integrated with centralized management solutions for all services.
2.7.1	**Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C**	Eclypsium provides authoritative device/firmware posture (inventory, integrity, drift, risk posture, and compliance) used for enforcement/monitoring. Eclypsium also provides advanced threat detection not available in traditional virus checkers.

ID #	Activity Name	How Eclypsium Supports the Activity
2.7.2	**Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1**	Eclypsium extends XDR capabilities below the operating system, providing the hardware-level telemetry and behavioral analytics needed to detect threats that traditional cross-pillar tools miss.
Application & Workload		
3.1.1	**Application/Code Identification**	Eclypsium provides authoritative device/firmware posture (integrity, vuln, supply chain risk) used for enforcement/monitoring. Eclypsium also provides a patch management capability for devices.
3.2.1	**Build DevSecOps Software Factory Pt1**	Eclypsium provides supporting posture signals, and patch management capabilities utilized in development pipelines
3.3.1	**Approved Binaries/Code**	Eclypsium provides authoritative device/firmware posture (integrity, vuln, supply chain risk) used for enforcement/monitoring. Eclypsium also provides a xBOM integration of firmware.
3.3.2	**Vulnerability Management Program Pt1**	Eclypsium provides vulnerability management by identifying and prioritizing firmware vulnerabilities and insecure configurations across the device fleet, including exposures not visible to OS only scanners.
3.3.3	**Vulnerability Management Program Pt2**	Eclypsium supports vulnerability management by identifying and prioritizing firmware vulnerabilities and insecure configurations across the device fleet, including exposures not visible to OS-only scanners. These findings can be integrated into enterprise vulnerability management programs through Eclypsium's integration suite of tools.
3.3.4	**Continual Validation**	Eclypsium provides continual validation by continuously verifying firmware integrity and baseline compliance, and by alerting on drift or newly discovered vulnerabilities and threats that impact device trust.
Automation and Orchestration		
6.1.1	**Policy Inventory & Development**	Eclypsium supports policy inventory and development by providing measurable, continuous evidence of device and firmware trust (inventory, integrity baselines, vulnerability exposure, patch currency) that Components can map to existing standards and identify gaps.
6.7.1	**Workflow Enrichment Pt1**	Eclypsium supports workflow enrichment by supplying high-value device and firmware context (integrity status, baseline drift, exploit exposure, patch posture) to IR/IT workflows in SIEM/SOAR/ITSM tools.
6.7.2	**Workflow Enrichment Pt2**	Eclypsium supports workflow enrichment maturation by enabling consistent device-trust context to be attached to incidents and tickets and used for prioritization and recommended actions (e.g., quarantine, update, isolate).
Visibility and Analytics		
7.3.1	**Implement Analytics Tools**	Eclypsium provides analytics implementation by acting as a specialized telemetry source for device and firmware trust, feeding integrity, vulnerability, and patch posture data
7.3.2	**Establish User Baseline Behavior**	Eclypsium ensures that behavior driven analytics are built on a foundation of trust by verifying the integrity of the device and establishing NPE/device baselines. Coupled with the Automata engine, Eclypsium flags NPEs/devices that deviate from their known-good baseline or expected operating patterns.

ID #	Activity Name	How Eclypsium Supports the Activity
7.5.1	**Cyber Threat Intelligence Program Pt1**	Eclypsium supports a cyber threat intelligence program by providing firmware-focused threat and vulnerability intelligence (affected platforms, exposure indicators, and remediation guidance) that can be incorporated into CTI and prioritization workflows
7.5.2	**Cyber Threat Intelligence Program Pt2**	Eclypsium supports CTI program maturation by continuously updating firmware risk intelligence and producing actionable device-level findings that can be correlated with other threat sources in SIEM/XDR/CTI tooling.